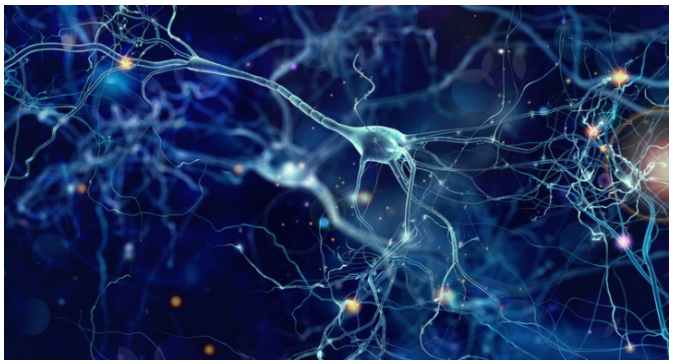
WARD AND SMITH, P.A.
ATTORNEYS AT LAW

# Healthcare Highlights: Cyber-Security, Licensing Board Issues, and Employer COVID-19 Regulations

**Written By** **Leigh A. Wilkinson** (law@wardandsmith.com)
December 3, 2021



**Recently, several Ward and Smith attorneys held a Health Care Breakfast and Learn to provide insights on the healthcare industry relevant to their specific areas of expertise, from privacy and data security to professional licensing issues and labor and employment.**

### Privacy and Data Security

Peter McClelland, a privacy, data security, and technology attorney who is also a Certified Information Privacy Professional, began the discussion with some trends and tips for healthcare providers to be aware of in regards to cybersecurity.

"Healthcare and financial services are always neck and neck each year for which industry in the United States gets targeted the most by malicious cyber actors," said McClelland.

In the world of data security, there are three major trends that have been especially relevant to healthcare providers over the past few years:

- Substantial increase in cyberattacks - malicious actors using trusted third parties or managed service providers to gain access to computer systems and personal information
- Significant uptick in the sophistication of cyberattacks - phishing schemes, tiny changes in email addresses, and spoofed email accounts increasingly difficult to identify
- Increased costs associated with successful attacks - average cost for a data breach in 2020 was around $4 million

Outside of the healthcare industry, an attack on a managed service provider, service partner, or supplier is typically referred to as a supply chain attack. These supply chain attacks are the ones that have made headlines in recent years, with companies such as Colonial Pipeline, Microsoft, and Cassia experiencing significant costs to their finances and brand reputation.

"When you read or hear about any of these things in the news, it can be easy to think that events are only tangentially relevant to you," explains McClelland, "but the same techniques in all of those get repurposed against entities in the healthcare space every day, whether they make headlines or not."

McClelland reported that phishing scams in prior years almost seemed to be deliberately obvious in terms of sophistication. Formerly, the most advanced phishing and ransomware technology was mostly just available to nation-states, but now it has become much easier for malicious cyber-actors and criminal organizations to implement it broadly to smaller companies.

The cost of dealing with a cyber-attack has skyrocketed as well. These are not just financial costs associated with remediation, regulatory penalties, and brand damage but also include measurable losses in customer return and measurable losses from employee turnover.

To illustrate what could happen in a healthcare setting, McClelland referenced a study that put the average cost per patient record at $146. "In this example, if a physician's office kept a record including a patient's name, sex, age, phone number, email address, and insurance, that would be six records. At $146 per record, with six records per patient, the expected cost per patient would be around $876, so if a business had 1,000 patients in a breached system, you're looking at an estimated cost of $876,000."

### Risk Mitigation

As the frequency of these attacks is only increasing, training employees is an important means of limiting risk exposure, advised McClelland. He also recommends reviewing existing security and privacy policies to close gaps and ensure there is an incident response plan in place.

Having a security incident response program, and a training regimen to help employees understand how to use it, is known as an effective means of reducing the average cost of a data breach. McClelland also pointed out that the incident response plan should say who does what, when they should do it, with whom they need to consult, and in what order actions need to be taken when a security incident is suspected or confirmed.

"This should be printed out and distributed to everyone whose name is listed in the plan," notes McClelland, "because by definition, if you have a ransomware attack, you can't access any of your information on a computer system. It won't do you any good if the information is on the computer, and the computer is no longer accessible."

There are two other important things for healthcare organizations to consider in regards to analyzing the viability and effectiveness of their cyber-security:

- Review scope of contracts with managed service providers – understand the nature of relationships with business partners and customize risk allocation between parties
- Incorporate cyber-liability insurance into existing business practices

"Cyber-liability insurance is not a substitute for having a robust privacy and security program in the same way that health insurance is not a substitute for diet and exercise," added McClelland. To get a reduction on premiums, he recommends incorporating good privacy and security protections.

### Licensing Board Issues

Troy Smith, a business law attorney with over 50 years of experience, provided guidance and practical tips for how licensees in a healthcare environment should respond to issues and inquiries from licensing boards. Smith initiated the discussion by advising licensees to understand that a license is not a right; instead, it is a privilege.

"Do not let the licensees in your organization forget that it is a lot easier for a licensing board to limit or take a license than it was for a licensee to earn it," Smith commented.

There are many things for licensees to be aware of prior to responding to a licensing board and numerous professional standards that need to be adhered to in order to keep a license. Professional standards have little to do with the skill set of an individual, and the framework surrounding these standards is constantly in flux.

Licensing boards are well-staffed, and the individuals are highly experienced, said Smith. "They deserve respect, and your licensee needs to provide that respect if they have an encounter," he said. "They can truly be your licensee's best friend or worst enemy."

According to Smith, an inquiry from a licensing board is generated in one of two ways:

- Self-disclosure - often disclosed on licensing applications, renewals, or conditionally due to the recognition that an unfortunate situation from the applicant's past will be uncovered
- Patient complaints - most frequent cause of inquiries from licensing boards

Whether a result of a DUI charge, disorderly conduct, or some other negative incident from an individual's past, licensees should seek assistance from an attorney when dealing with self-disclosure, Smith says. Also, considering that most licensing boards have guidance about how to file a complaint prominently displayed on their websites, which makes it easy for patients to do that, a licensee should never treat an inquiry from their licensing board as a matter of routine.

Smith pointed out that, "These are big stakes, and that license is hanging in the balance. The number one thing to do before the licensee responds in any way or does anything is to consult a lawyer." It is also critical to avoid the attitude of saying, "I didn't do anything wrong. I want to be helpful and friendly. I will just talk to the medical board; I'll talk to their investigator," noted Smith.

Engaging the services of a qualified attorney is essential for licensees, as the attorney acts as a tour guide and bodyguard in discussing facts, editing, and crafting responses. Going into a situation without any help and/or failing to heed the advice of an attorney is inadvisable; lying to the medical board is equivalent to a death sentence.

"If you're getting the impression that your licensing board is the policeman, the district attorney, the judge, jury, and executioner, you're right," added Smith.

#### Employment Law and COVID-19

Ken Gray, a labor and employment attorney who leads Ward and Smith's labor and employment practice group, provided attendees with a deep dive into the emergency temporary standard (ETS) that OSHA issued in June of 2021 as a response to the Coronavirus pandemic.

Essentially, the healthcare ETS applies, with some exceptions, to settings where employees provide health care services or health care support services, such as billing insurance, human resources, and healthcare facilities. The ETS does not apply to:

- The provisions of first aid by an employee who is not a licensed healthcare provider
- Pharmacists in retail settings
- Non-hospital ambulatory care settings where all non-employees are screened prior to entry and excluded from entry if they have COVID-19 symptoms
- A well-defined hospital ambulatory care setting where all employees are fully vaccinated, all non-employees are screened prior to entry, and people who are suspected as having COVID-19 or who have tested positive are not permitted to enter that particular facility

- Home health care settings where all employees are fully vaccinated and all non-employees are screened and not permitted if they are suspected or confirmed
- Telehealth services performed outside of a setting where direct patient care occurs
- Support services provided in a different facility than where the patients are staying

People can apply for an exemption to mandatory vaccination policies because of a legitimate medical reason, a religious belief, or disability. One of the key requirements of this ETS is that employers must have a written COVID-19 plan.

Gray mentioned that "[I]f someone turns you over to OSHA and you do not have a plan in place, you will be cited, and it will have a monetary component to it." For providers with multiple facilities, there should be a plan for each facility, and each site should have its own workplace safety coordinator.

Each plan should be monitored to ensure it is effective and identify necessary updates, said Gray. Also, the plan should include policies and procedures to minimize the risk of transmission of COVID-19, as well as strategies for limiting and monitoring points of entry to settings where direct patient care is provided. Employers should also provide and ensure employees wear face masks indoors, advised Gray.

There are many requirements pertaining to notifying an employee if they have been in the presence of someone that's COVID-19 positive. "If one of your employees is exposed to someone at work and they need to go get tested, it is the employer's responsibility to pay for that test," Gray explained.

Even if an employee is out for months due to COVID-19, it is not permissible to terminate them. The ETS also requires employers to continue providing benefits to which the employee is normally entitled and to pay the employee the same regular pay and benefits they would have received had the employee not been absent from work, up to $1400 per week for, at least, the first two weeks.

The ETS is extremely complicated, and Gray expects that "[t]here will be lawsuits. And we'll have to see what those lawsuits accomplish. But, the health care ETS is in effect."

--